

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Общая алгебра

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности..

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1. Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин, которые обеспечивают возможность решения задач профессиональной деятельности.

ИОПК-3.2. Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности.

ИОПК-3.3. Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– контрольная работа.

Примеры задач

1. Найти $d = \text{НОД}(a, b)$ и разложение $d = au + bv$ для двух чисел: 150 и 84. 4. Найти НОК двух чисел: 150 и 84.

2. Найти функцию Эйлера для числа 21.

3. Найти остаток от деления 5^{1202} на 13

4. Найти остаток от деления 8559 на 11

5. Найти наименьшее натуральное число, удовлетворяющее системе сравнений:

$$\begin{cases} x \equiv 1(3) \\ x \equiv 2(5) \\ x \equiv 1(7) \end{cases}$$

6. Умножить $(2 + i)(1 + 2i)$

7. Вычислить $\frac{-6 + 4i}{2 + 3i}$

8. Решить систему уравнений в поле вычетов Z_5
$$\begin{cases} 4\bar{x} + 3\bar{y} = \bar{1} \\ 2\bar{x} + \bar{1}\bar{y} = \bar{3} \end{cases}$$

9. Поделить с помощью схемы Горнера в поле R : $f(x) = x^3 + 2x^2 + 8x + 12$ на $g(x) = x - 3$

10. Поделить с помощью схемы Горнера в поле Z_5 : $f(x) = x^3 + 2x^2 + 3x + 4$ на $g(x) = x + 3$

11. Найти НОД двух многочленов $f(x) = x^3 + 11x^2 + 34x + 24$, $g(x) = x^2 + 8x + 12$.

12. Найти НОД и коэффициенты Безу для $f(x) = x^3 + 6x^2 + 13x + 10$, $g(x) = x^2 + 5x + 7$.

13. Найти многочлен 3-й степени, если: $f(-1) = 3$, $f(0) = 3$, $f(1) = 7$, $f(2) = 21$ (интерполяция, метод неопределённых коэффициентов либо Лагранжа).

14. Выполните разложение $f(x) = x^4 + 5x^3 + 9x^2 + 7x + 2$ на неприводимые многочлены с помощью метода Кронекера.

15. Найдите кратные корни и выполните разложение на неприводимые многочлены в поле R с помощью НОД многочлена и его производной (либо с помощью матрицы Сильвестра): $f(x) = x^3 - 4x^2 + 5x - 2$.

16. Найти результат двух многочленов с помощью определителя Сильвестра $f(x) = x^2 + x + 5$ $g(x) = x^2 + 2$.

17. Какими свойствами обладает бинарная алгебраическая операция $< \square, * >$, где $a*b = \sqrt{a^2 + b^2}$.

18. Пусть $G = \square \setminus \{0\}$, $<G, \cdot>$, $G' = \{g^n \mid n \in \square\}$, g – фиксированный элемент из G . Будет ли G' подгруппой группы G ?

19. Какими свойствами обладает бинарная алгебраическая операция $< \square, * >$, где $a*b = 4ab$.

20. Пусть $G = M(2, \square)$, $<G, +>$, $G' = \left\{ \begin{pmatrix} a & b \\ ab & a \end{pmatrix} \right\}$ (где $\forall a, b \in \square$). Будет ли G' подгруппой группы G ?

21. Пусть $K = M(2, \square)$, $K' = \left\{ \begin{pmatrix} a & b \\ -b & 0 \end{pmatrix} \right\}$ (где $\forall a, b \in \square$). Будет ли K' подкольцом кольца K ?

22. С помощью многочлена $f(x) = x^2 + x + 2$ построить расширение поля $GF(3)$.

23. Пусть $P = \square$, $P' = \{2\alpha + 3\beta \mid \forall \alpha, \beta \in \square\}$. Будет ли P' подполем поля P ?

24. С помощью многочлена $f(x) = x^2 + 2x + 2$ построить расширение поля $GF(3)$.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Экзамен в третьем и четвертом семестрах проводится в письменной форме по билетам, билет состоит из 2 теоретических вопросов. Продолжительность экзамена 1,5 часа. Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». За верный ответ по теории студент получает 1,5 балла из 5 баллов оценки. При сложении с семестровым рейтингом за практику (3,5 балла из итоговой оценки) студент получает 5,0 баллов. В случае получения дробной оценки, итоговая оценка определяется по правилам округления.

Примерный перечень теоретических вопросов

Кольца и поля

Определение кольца; теорема об основных соотношениях в кольце.

Кольцо многочленов.

Определение поля; 2 примера поля.

Кольцо классов вычетов по идеалу.

Понятие делимости и алгоритм деления Евклида для целых чисел.

Кольцо классов вычетов целых чисел; доказать, что совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому целому числу.

Кольцо классов вычетов целых чисел.

Кольцо классов вычетов целых чисел. Простые поля Галуа.

Полная и приведенная система вычетов (с примерами).

Функция Эйлера. Теорема о мультипликативности функции Эйлера.

Системы сравнений. Китайская теорема об остатках.

Многочлены над полем: нормированный многочлен, неприводимый многочлен, теорема деления для многочленов, алгоритм деления Евклида для многочленов.

Теорема Безу (с доказательством).

Идеал в кольце многочленов; сформулировать три теоремы для кольца многочленов, аналогичные теоремам для идеала в кольце целых чисел. Определения расширения и характеристики поля Галуа.

Доказать, что в поле характеристики p имеет место равенство $(a + b)^p = ap + bp$.

Минимальная функция; 2 теоремы о свойствах минимальной функции (с доказательством).

Определение системы линейных уравнений над полем; совместные и несовместные системы; однородные и неоднородные системы.

Примитивный элемент в поле Галуа. Дискретное логарифмирование в полях Галуа.

Метод решения однородной системы линейных уравнений над полем.

Доказать формулы умножения и деления в тригонометрической форме

$$\rho_1 \rho_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)) \quad \frac{z_1}{z_2} = \frac{\rho_1}{\rho_2} (\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2)) .$$

Доказать формулу Эйлера $e^{ix} = \cos x + i \sin x$.

Доказать формулу Муавра $z^n = \rho^n (\cos(n\varphi) + i \sin(n\varphi))$

Доказать, что $\sqrt[n]{z} = \sqrt[n]{\rho} \left(\cos \frac{\varphi + 2\pi k}{n} + i \sin \frac{\varphi + 2\pi k}{n} \right)$

Доказать, что множество всех корней степени n из 1 является абелевой группой.

Доказать, что $\langle U_n, \cdot \rangle \cong \langle Z_n, + \rangle$ (группа корней степени n из единицы изоморфна аддитивной группе вычетов по модулю n).

Доказать, что если ε_k первообразный корень n -й степени из 1, то $(k, n) = 1$.

Доказать, что если $(k, n) = 1$, то ε_k первообразный корень n -й степени из 1.

Доказать, что сумма всех корней степени n из 1 равна 0.

Доказать, что $\cos z = \frac{e^{iz} + e^{-iz}}{2}$, $\sin z = \frac{e^{iz} - e^{-iz}}{2i}$.

Доказать, что $Ln(z) = \ln \rho + i(\varphi + 2\pi k) \quad (\forall k \in \mathbb{Z})$

Доказать теорему о делении с остатком: Для любых $a, b \in \mathbb{Z}, b \neq 0$ найдутся $q \in \mathbb{Z}$, $0 \leq r < |b|$, что $a = bq + r$. Причём q, r находятся единственным образом.

Доказать, что 2 числа имеют одинаковые остатки от деления на $m \Leftrightarrow (a - b) \text{ делится на } m$.

Доказать, что если $d = \text{НОД}(a, b)$, то существуют такие $u, v \in \mathbb{Z}$, что $d = au + bv$ (коэффициенты Безу).

Доказать, что для того, чтобы a, b были взаимно простыми, необходимо и достаточно существование целых чисел $u, v \in \mathbb{Z}$, таких что $au + bv = 1$.

Доказать, что если произведение двух целых чисел ab делится на целое число c , и первый множитель a взаимно прост с c , то $b \in \mathbb{M}$.

Доказать, что последний ненулевой остаток, полученный в алгоритме Евклида, является общим делителем для a, b .

Доказать, что последний ненулевой остаток, полученный в алгоритме Евклида, является наибольшим общим делителем a, b .

Докажите рекурсивные формулы для коэффициентов Безу: $u_k = u_{k-2} - q_k u_{k-1}$,
 $v_k = v_{k-2} - q_k v_{k-1}$.

Доказать, что все решения диофантового уравнения $ax + by = c$, где $a, b, c \in \mathbb{Z}$ задаются формулой
$$\begin{aligned} x &= uc - bk \\ y &= vc + ak \end{aligned} \quad (k \in \mathbb{Z}),$$
 где u, v коэффициенты Безу для a, b .

Докажите, что для любого простого $p \geq 5$ верно $p \equiv \pm 1 \pmod{6}$.

Докажите, что всякое натуральное число, большее 1, делится по крайней мере на одно простое число.

Докажите теорему Евклида о бесконечности множества простых чисел.

Докажите, что если $n \in \mathbb{N}$ не делится ни на одно простое число, меньшее или равное $\lfloor \sqrt{n} \rfloor$, то оно простое.

(Основная теорема арифметики). Доказать, что всякое натуральное число $n > 1$ может быть представлено в виде произведения простых чисел: $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, две таких записи могут отличаться лишь порядком следования сомножителей.

Докажите, что если $a = p_1^{s_1} \cdot \dots \cdot p_m^{s_m}$, $b = p_1^{t_1} \cdot \dots \cdot p_m^{t_m}$, то $\text{НОД}(a, b) = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$, где $k_i = \min(s_i, t_i)$, $\text{НОК}(a, b) = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$, где $k_i = \max(s_i, t_i)$.

Докажите формулу взаимосвязи НОД и НОК: $[a, b] = \frac{ab}{(a, b)}$.

Докажите универсальный признак делимости.

Доказать, что если старший коэффициент многочлена $g(x)$ обратим, то любой многочлен $f(x)$ можно разделить на $g(x)$ с остатком.

Доказать, что остаток от деления многочлена $f(x)$ на $x - a$ равен $f(a)$. В частности, a является корнем многочлена $\Leftrightarrow f(x) \in \mathbb{M}[x - a]$.

Доказать, что последний ненулевой остаток в алгоритме Евклида является наибольшим общим делителем двух многочленов.

Доказать, что кольцо K коммутативно $\Leftrightarrow$ кольцо многочленов $(K[x], +, \cdot)$ коммутативно.

Доказать, что кольцо K не содержит делителей нуля $\Leftrightarrow$ кольцо $(K[x], +, \cdot)$ без делителей нуля.

Доказать, что если многочлены взаимно просты попарно, то они взаимно просты в совокупности.

Доказать формулу взаимосвязи НОК и НОД: $[f, g] = \frac{fg}{(f, g)}$.

Доказать, что если многочлен степени $n \geq 2$ неприводим в поле P , то он не имеет корней в поле P .

Доказать основную теорему о разложении многочлена на неприводимые множители.

Доказать формулу вычисления определителя Вандермонда.

Доказать, что если в поле P есть n попарно различных элементов $\alpha_1, \dots, \alpha_n$, то для любых $\beta_1, \dots, \beta_n \in P$ существует единственный многочлен $f(x) \in P[x]$, такой, что $f(\alpha_i) = \beta_i \quad \forall i = 1 \dots n$.

Доказать, что многочлен степени $k > 0$ над полем P имеет не более k корней в этом поле.

Доказать интерполяционную формулу Лагранжа.

$$y = \sum_{i=1}^n y_i \frac{(x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n)}{(x_i - x_1) \cdot \dots \cdot (x_i - x_{i-1})(x_i - x_{i+1}) \cdot \dots \cdot (x_i - x_n)}$$

Вывести интерполяционную формулу Лагранжа для $n=2$ из канонического уравнения прямой.

Интерполяция Эрмита: доказать, что по значениям f и f' в 2 точках можно построить единственную кубическую параболу, которая совпадает с указанной функцией и имеет общую касательную с ней в этих двух точках.

Доказать, что если c является корнем кратности k для $f(x)$, то он является корнем кратности $k-1$ для $f'(x)$.

Доказать, что всякий многочлен степени $n \geq 1$ с комплексными коэффициентами имеет n корней (если учитывать их столько раз, какова кратность корня).

Доказать теорему Виета о взаимосвязи корней с коэффициентами многочлена.

Доказать, что если комплексное число z является корнем многочлена $f(x) \in R[x]$, то и $\bar{z}$ является корнем (той же кратности, что и z).

Доказать, что всякий многочлен нечётной степени с действительными коэффициентами имеет хотя бы один действительный корень

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ - многочлен с целыми коэффициентами.

Если $\frac{p}{q}$, где $p \in \mathbb{Z}, q \in \mathbb{N}$, является корнем многочлена $f(x)$, то: 1) $a_n \nmid p$, 2) $a_0 \mid p$.

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ - многочлен с целыми коэффициентами.

Если $\frac{p}{q}$, где $p \in \mathbb{Z}, q \in \mathbb{N}$, является корнем многочлена $f(x)$, то $f(m) \equiv 0 \pmod{p - mq}$ для любого целого m .

Для каждого ненулевого многочлена $f(x) \in \mathbb{Q}[x]$ с рациональными коэффициентами существует ассоциированный с ним примитивный многочлен с целыми коэффициентами, $f(x) \in \mathbb{Z}[x]$.

Лемма Гаусса. Произведение примитивных многочленов есть примитивный многочлен.

Теорема Эйзенштейна. Если для многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ с целыми коэффициентами существует простое число p , удовлетворяющее условиям:

- 1) a_n не делится на p .
 - 2) $a_{n-1}, \dots, a_2, a_1, a_0$ делятся на p .
 - 3) a_0 не делится на p^2 .
- то $f(x)$ неприводим над полем $\mathbb{Q}$.

Докажите одну из формул представления результата: $R(f, g) = a_n^s \prod_{i=1}^n g(\alpha_i)$,

$$R(g, f) = b_s^n \prod_{j=1}^s f(\beta_j)$$

Докажите, что результат равен определителю матрицы Сильвестра.

$$D(f) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Доказать взаимосвязь между дискриминантом и

$$\text{результантом: } R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f).$$

Доказать, что замена $x = y - \frac{b}{3a}$ сводит многочлен 3 степени $ax^3 + bx^2 + cx + d$ к виду, не содержащему 2-й степени.

Доказать, что дискриминант уравнения $x^3 + px + q = 0$ равен $D = -4p^3 - 27q^2$.

Доказать, что $\alpha + \beta$ является корнем уравнения $x^3 + px + q = 0$, где

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Доказать, что счётное множество счётных множеств счётно и что Q тоже счётно.

Доказать, что множество всех подмножеств счётного множества не является счётным (теорема Кантора) и что интервал $(0,1)$ не является счётным.

Теорема Кантора-Бернштейна. Если множество A равномощно подмножеству множества B , а B равномощно подмножеству множества A , то A и B равномощны.

Вывести формулы числа размещений и сочетаний $A_n^m = \frac{n!}{(n-m)!}$ $C_n^m = \frac{n!}{m!(n-m)!}$

Вывести формулу числа сочетаний с повторениями $\tilde{C}_n^m = C_{n-1+m}^{n-1} = \frac{(n-1+m)!}{m!(n-1)!}$

Доказать свойство Паскаля. $C_n^k + C_n^{k-1} = C_{n+1}^k$.

Доказать, что C_n^m это коэффициенты бинома Ньютона $(a+b)^n$.

Вывести формулу субфакториала $!n = n! \left(\frac{1}{2!} - \frac{1}{3!} - \dots + (-1)^n \frac{1}{n!} \right)$.

Вывести рекурсивную формулу $!(n+1) = n \cdot (!n + !(n-1))$.

Числа Стирлинга 2 рода: число разбиений n -элементного множества на k подмножеств. Вывод формулы $S(n, k) = S(n-1, k-1) + S(n-1, k) \cdot k$.

Числа Стирлинга 1 рода: число перестановок порядка n с k циклами. Вывод формулы $c(n, k) = c(n-1, k-1) + (n-1) \cdot c(n-1, k)$.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Для проверки остаточных знаний можно использовать задачи из типовых контрольных работ, выполнявшихся в течение семестра (приведены в пункте 2).

Информация о разработчиках

Приходовский Михаил Анатольевич, канд. физ.-мат. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.